Next VVSG Training
Security: Testing Requirements

October 15-17, 2007

Nelson Hastings
National Institute of Standards and Technology
nelson.hastings@nist.gov

Agenda

- Review of security related part of Chapter 2: Conformity Assessment Process
- Review of Section 5.5 Open Ended Vulnerability Testing (OEVT)

Chapter 2: Conformity Assessment Process

- Section 2.4.3: Initial System Build by Test Lab
- Section 2.4.4: Unmodified COTS Verification
- Section 2.6.1.1: Voting System Software Version
- Section 2.6.2: Software Distribution Requirements for Repositories, Test Labs, and Manufacturers

2.4.3 Initial Build by Test Lab

- The process used by test labs to build of voting system software
  - Known as the “witness build” or “trusted build” in previous standards
- Based on the “Testing and Certification Program Manual” from the EAC

2.4.3 Initial Build by Test Lab

- Performed by lab personnel and witnessed by manufacturer personnel
- Two step process
  - Establishment of build environment used to create voting system software
  - Build of voting system software using established build environment
    - Initial build of software
    - Update of previously built software

2.4.3 Initial Build by Test Lab

- Build environment establishment and voting system software build
  - TDP contains procedures
  - Digital signature verification of voting system software; and when possible components of build environment
  - Document procedures used
  - Digitally signed binary image of build environment and built software on unalterable media

2.4.3 Initial Build by Test Lab

- Update of previously built software
  - Establish the build environment and previously built software from unalterable media
  - Place update source code onto the build environment after digital signature verification.
  - Build software based on procedures in TDP

2.4.3.4 Unmodified COTS Verification

- The process used by test labs to verify COTS products have not been modified
  - Manufactures provide documented procedures to assemble and configure COTS products used in voting systems
  - Test labs obtain COTS products from the open market

2.4.3.4 Unmodified COTS Verification

- Test labs assemble and configure COTS products into the voting system
  - Witnessed by manufacturer personnel
  - The procedures used assemble and configure COTS into voting system documented

2.6.1.1 Voting System Software Version

- Identifies the version of the voting system software to be used as part of voting system recommended for certification
  - If no updates or modifications occurs since the initial test lab build, use the initial build
  - When updates and modifications have occurred since the initial build, perform a final test lab build

2.6.2 Software Distribution

- Requirements for repositories, test labs, and manufacturers
  - Could be used by jurisdictions
- Traceability of software to a master software distribution package stored on unalterable media
- Records related to the creation of master copies and copies derived from a master copy

2.6.2 Software Distribution

- Characteristics of software distribution packages
  - Human readable file containing information (name, manufacturer, version, etc.) about each piece of software in the package
  - Digital signatures for each piece of software in the package
  - Labeling and digital signature requirements for each piece of physical media of a software distribution package

2.6.2 Software Distribution

- Repository requirements
  - Publicly documented process to request copies of software distribution packages
  - Receive software from test labs, national certification authorities, and jurisdictions
  - Digital signature validation before using software to create software distribution package master copies

2.6.2 Software Distribution

- Three types of repositories
  - Notary repositories distribute integrity information of software
  - Escrow repositories hold software until formally requested
  - Distribution repositories provide software to parties approved by the software owner

2.6.2 Software Distribution

- Test lab requirements
  - Create software distribution package master copies containing
    - Voting system source and executable code
    - Configuration files, installation programs, and third party software
    - Provide copies to manufacturer and designated national repositories including the NSRL
  - Copies of the build environment provided to the manufacturer and designated national repositories including the NSRL

2.6.2 Software Distribution

- Manufacturer requirements
  - Create software distribution package master copies containing
    - Source code of voting system software
    - Configuration files, installation programs, and third party software
    - Provide copies of the software distribution packages as part of the TDP

5.5 Open Ended Vulnerability Testing (OEVT)

- What is Opened Ended Vulnerability Testing?
- What will the test labs actually DO?
- Why has OEVT been added?
- How will OEVT help?

OEVT is an attempt to...

- Bypass the security of a system
- Discover flaws that could be used to
  - change the outcome of an election,
  - interfere with voters' ability to cast ballots or have their votes counted
  - compromise the secrecy of the vote

OEVT is not ...

- A way to prove that a system is secure
- Bound by a pre-determined test plan

The test team will ...

- Figure out how the system works
- Identify the vulnerabilities – actual and potential
- Attempt to break-in using a variety of different approaches

Important Note

- Specific findings may differ
  - Labs may test aspects of the system in different orders
  - Labs can stop testing at any point after finding significant flaws
- Consistent framework for discussing critical flaws
  - Context of specific implementations
  - Corresponding plausible threat scenarios

5.4 Open ended vulnerability testing (OEVT)

- 5.4.1 Scope and priorities
- 5.4.2 Resources and level of effort
- 5.4.3 Rules of engagement
- 5.4.4 Fail criteria
- 5.4.5 Reporting requirements
- 5.4.6 VSTL response to OEVT

5.4.1 Scope and priorities

Open ended vulnerability testing will

- Encompass voting system and manufacturer supplied use procedures
- Focus on major flaws
- Pass/fail testing based on security models as implemented to address plausible threat scenarios

5.4.2 Resources and level of effort

- Team will be made up of security and election management experts
- Minimum of 12 staff weeks
- Team will be given a voting device, its TDP and the user documentation
- Team will also be given any available test data

5.4.3 Rules of engagement

- Team must examine system within the context of a process model with plausible threats
- Team must be given a description of the system as it is to be implemented
- Team must be given a description of how significant threats are addressed

5.4.4 Fail criteria

Reasons that a VSTL would recommend a fail include:

- A violation of mandatory VVSG requirements
- Inadequate means to mitigate a significant, known threat
- A critical flaw

5.4.5 Reporting requirements

Teams must include in their final report all information associated with test to include

- Threat scenarios considered
- Threat scenarios identified but not investigated
- Discussion of remaining vulnerabilities
- Team qualifications and each individuals' level of effort

5.4.6 VSTL response to OEVT

VSTL will review findings in light of all other test results.

By adding OEVT ...

- Labs may catch unanticipated design or implementation vulnerabilities
- Efficiency may improve for testing certain requirements

Security: Testing Requirements End

Questions?